TAT

CENTRAL INTELLIGENCE AGENCY
Office of Legislative Counsel
Washington, D. C. 20505
Telephone: [redacted]

30 July 1976

TO: Mr. Fred Asselin
Senate Government Operations Committee
3308 New Senate

Attached is a draft report of the development of the security programs for our computer systems which we would incorporate in our written response to your letter from the Committee.

Your comments will be most appreciated.

TAT

[redacted]
Assistant Legislative Counsel

Attachment

FORM 6-68 1533 OBSOLETE PREVIOUS EDITIONS (40)

DRAFT

The Central Intelligence Agency has been aware of the risks associated with automatic data processing (ADP) and computers from their initial application within the Agency to the present. This awareness was, and continues to be, based on the potential loss/disclosure, manipulation/change, or accidental/malicious destruction of National Security information or the software and hardware used to process or store this information. The DCI is charged with the protection of this information by various legislations, Executive Orders, and other appropriate regulations and directives. Examples of these are: the CIA Act of 1949; The National Security Act of 1947; E.O. 11652; E.O. 11905; The Privacy Act of 1974; and National Security Council Directives.

The Agency's computer security program was formalized in 1967 as a unique security discipline and has advanced and grown with the advancement and growth of the Agency's computer operations. The underlying and fundamental goal of the Agency's security program is the protection of information. The computer, as a processor or handler of information, must, therefore, be protected at the same level as the information it is processing. In addition,

high security standards are required because of the storage and availability of large quantities of information within a computer system and the relative ease with which this information can be retrieved or manipulated. The Agency's computer security program has evolved as a combination of the traditional security concepts of Personnel Security, Physical and Technical Security, and Procedural Security with the concepts of Hardware, Software, and Data Security.

These concepts establish personnel integrity, legitimate and authorized access to information and its use, and conversely protection against unauthorized or illegitimate use or access.

Some specific security features of our computer security program are:

1. Only personnel having an Agency Top Secret clearance and specific and legitimate need, will be authorized to access or use Agency computer resources.

2. Security features in computer hardware and software are applied to restrict the computer user to his legitimate and authorized needs

3. Security indoctrination and education of all employees is a continuous process.

4. Computer security policy has been established and is operational.

5. A high level of physical security is maintained throughout all Agency installations, with computer areas receiving additional protection.

6. The security posture of Agency computer operations is under continuous scrutiny by a group of professional Computer Security Officers.

In addition to the computer security program at CIA, an ADP Audit Staff, reporting to the Inspector General, was established in 1969. Initially, the attention of this Staff was focused on automated computer systems in the administrative areas of CIA. Examples of systems of major concern are payroll, general accounting, inventory control, and personnel. This Staff now plans to extend its audits to all major computer systems in CIA. In addition to periodic reviews of indiviual systems, the ADP Audit Staff conducts audits of individual computer installations in CIA to ensure proper management controls over computer technology.

Discussions with ADP auditors and managers in private industry and other government organizations, including GAO, have convinced us that CIA's approach to ADP auditing is correct. The ADP auditor at CIA monitors computer systems during design and development as part of a team. This team includes the end user, the ADP professional, and the ADP auditor. CIA auditors and ADP professionals agree that it is more difficult and expensive to correct build-in weaknesses after a system is operational than to eliminate the weaknesses in the progressive stages of development and testing.

CIA's program, then, is based on a close working relationship among a group of trained and responsible ADP professionals, an independent group of computer security professionals, and

an independent group of ADP auditors. This ongoing program is continually monitored and improved to ensure that it remains effective. CIA is confident that this program provides reasonable safeguards against the computer abuses covered in the recent GAO reports.

Honorable Abraham Ribicoff
United States Senate
Washington, D.C. 20510

Dear Senator Ribicoff:

In response to your request for Central Intelligence Agency assistance to the Senate Government Operations Committee investigation into the problems associated with the use of computer technology in the Federal Government, CIA representatives met with Committee Investigators Philip R. Manuel and Fred Asselin. The purpose of this meeting was to explore how CIA can assist the investigations without compromising the security methods CIA uses to protect intelligence. Naturally, CIA is reluctant to disclose in detail the security methods it uses to safeguard computer operations. This reluctance has the same basis as GAO's reluctance to identify specific installations where it discovered inadequate safeguards against computer damage. Such identification runs the risk that persons would attempt to exploit the implied security weaknesses and circumvent explicit safeguards.

CIA shares your concern in the areas of computer fraud, computer security, and automated decisionmaking computer applications. The enclosed documentation generally outlines CIA's approach to computer security. I hope it will be useful to your Committee, but I also hope that it will not result in CIA being used in some way as a model. Much of

the success we have had in preventing problems in the area covered by the three GAO reports can be attributed to the fact that at CIA, as in other national security organizations, computer technology has been introduced into a security conscious environment. The overhead of security is one of the prices we pay for doing business; it is an overhead we have learned to live with and, to some extent, embrace.

The safeguards and management controls we have applied to the use of computer technology have their price tags also. Those which we employ in the interest of national security may be too expensive for other Federal Government installations to jusitfy. Without belaboring the point, let it be fully admitted that tight security is expensive, but appropriate security is cheap when compared against the catastrophe associated with no protection whatsoever.

At CIA we have tried to build a balanced ~~system~~ program of security safeguards and management controls, ~~based~~ this program essentially follows ~~on~~ the general principles contained in AFIPS System Review Manual on Security (1974) the FIPS Guidelines for Automatic Data Processing Physical Security and Risk Management (1974) and standard auditing practices.

CIA endorses your Committee's efforts to make Federal managers aware of the need for such a ~~system~~ program.

Sincerely,

Attach: a/s

Next 1 Page(s) In Document Exempt

Approved For Release 2005/02/10 : CIA-RDP78M02660R000300020014-9

OLC #76-2437

15 SEP 1976

MEMORANDUM FOR: Legislative Counsel

ATTENTION : [redacted] ST

FROM : Robert W. Gambino
Director of Security

SUBJECT : "Problems Associated With the Increasing Uses of Computer Technology in the Federal Government" -- Preparation of a Draft CIA Response to the Senate Government Operations Committee

REFERENCES : a. Letter to DCI from Senator Abe Ribicoff, dated 21 May 1976, same subject

b. Letter to Senator Abe Ribicoff from DCI, dated 4 June 1976, same subject

c. Letter to [redacted] from Mr. Fred Asselin, dated 3 August 1976, same subject ST

d. Letter to [redacted] from Mr. Fred Asselin, dated 4 August 1976, same subject ST

1. Attached is a short draft paper concerning the Agency's Computer Security Program which the Office of Security has prepared. This paper is for use in preparation of a formal letter combining appropriate input from the Office of Data Processing, the Audit Staff, and the Office of Security in response to the references.

2. Please feel free to contact my representatives for further information or amplification of any parts of this paper.

[redacted] ST

Robert W. Gambino

Attachment

cc: AI/DDA

OS6-3991

Approved For Release 2005/02/10 : CIA-RDP78M02660R000300020014-9

D R A F T
7 September 1976

The Central Intelligence Agency has been aware of the risks and dangers associated with automatic data processing since its earliest application within the Agency. The Agency's Computer Security program is intended to minimize the risks of; unauthorized or accidental loss or disclosure of classified or sensitive information, alteration or manipulation of this information, and damage or destruction of this information or any portion of the ADP facility. It is believed that such a computer security program is a basic element in reducing the risks of information compromise and certain aspects of computer mismanagement by restricting access to computer resources to only duly authorized personnel.

The requirements for the protection of information which are the basis of the Agency's computer security program, are found in various Statutes, Executive Orders and Directives. They are:

To be inserted by O.L.C. with appropriate passages

Examples:

N.S.A. Act of 1947

CIA Act of 1949

E.O. 11652

E.O. 11905

N.S.C. Directives

Others as appropriate

DCID 1/16 - Classified

H.R. 10-19 - Classified

The Agency's computer security program was formalized in 1967 as a unique security discipline with the appointment of a Special Assistant for Automatic Data Processing within the Office of the Director of Security. Additional staffing was provided as the Agency's computer operation advanced and grew. At the present time, the Information Systems Security Group of the Office of Security develops and promulgates computer security policy, assists in implementation of this policy and, through a continuing review of computer operations, acts as an enforcement body. The Information Systems Security Group is staffed by both professional security officers and professional data processing personnel. This personnel mix provides for the best interchange and understanding of the complex computer security problems and solutions. In addition, this staffing for computer security allows responsiveness to the diversity of computer operations and security requirements.

The Agency's computer security program is a combination of the traditional security concepts of Personnel Security, Physical and Technical Security, and Procedural Security, with Computer Hardware, Software, and Data Security. These concepts and their implementation result in a selection of personnel with high personal integrity combined with procedures establishing legitimate and authorized access and use of the computer and its resources. An underlying and fundamental goal of the Agency's security program is the protection of information. It should be noted that computer security is but one aspect of the Agency's overall security environment. The computer, as a processor or handler of information, must therefore be protected at the same level as the information it is processing. In addition, high security standards are required because of the storage and availability of large quantities of information within a computer system and the relative ease with which this information can be retrieved and manipulated without appropriate controls.

The unique mission and environment of the CIA has required the establishment of high security standards for

all its activities to protect these activities from hostile penetration or destruction. Some specific security features which are supportive for the computer security program are:

1. Personnel

Historically, the Agency has always placed a great deal of emphasis on personnel security. All applicants are subject to a background investigation and polygraph examination to establist that they meet Agency security criteria. These criteria require that all employees be of "excellent character, and of unquestioned loyalty, integrity, discretion and trustworthiness." Information taken into consideration in determining whether an individual meets these standards is based on, but not limited to, the requirements outlined in Executive Order 10450. In making security clearance determinations, no one event in a person's past is viewed in isolation. The person's entire record is evaluated, and a decision is made based on the totality of that record, rather than on a specific incident which may or may not have been out of character with

the rest of this person's conduct. Under these procedures, all personnel hired by the Agency meet the requirements for a Top Secret clearance. This guarantees a high standard of personnel security for all employees used in computer operations by the Agency. Additionally, the Agency has a program under which employees are periodically reinvestigated to confirm that they continue to meet the same high standards as when they entered on duty. A final point is that the Agency personnel security program applies to all employees, no matter what their grade or position. This ensures that there is no one group of employees which is any more vulnerable to security compromise than any other group.

2. Physical Security

The Agency maintains a high degree of physical security protection for all its installations. Physical security can be viewed as protective rings or barriers surrounding an asset.

As the value of an asset or, conversly, the assessment of a perceived threat varies, so will the strength of the physical security of the assets. The nature of a computer facility in both value of equipment and data, establishes a high degree of physical security protecting these areas. Examples of physical security features employed are; physical locations, vaulted areas; controlled access, alarms, and established security procedures.

3. Hardware and Software

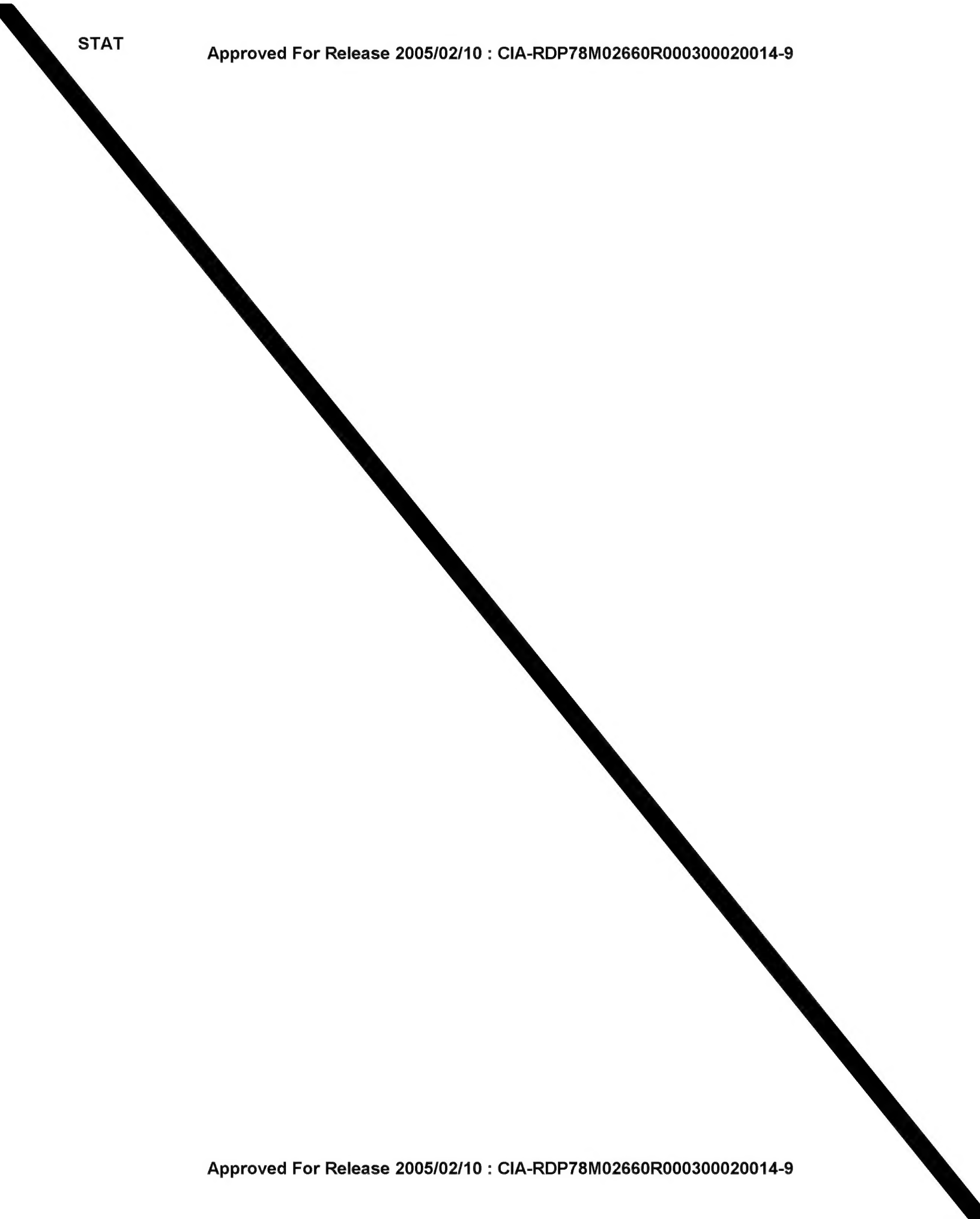
Computer hardware and the software utilized to operate them have been designed to provide certain forms of self-protection for the computer system and the data stored and processed by them. The Agency employs these protective features, where applicable, as an important and valuable security tool. As the awareness of computer vulnerability increases, and with a commensurate demand for security, it is believed the computer hardware and software security features will be emphasized.

4. Security Indoctrination

Security indoctrination and education of all Agency employees is a continuous process. Computer users are additionally provided security indoctrination through briefings, documentation, and notices concerning various computer security problems and features.

Due to its unique mission and environment, the costs of the Agency's security program are accepted as necessary. The computer security program is an integral part of the Agency's overall security program, and it is extremely difficult to cost out this as a separate program other than on a personnel basis. Overall cost factors would, however, at a minimum include personnel clearance, physical security, computer hardware and software, safety and contingency plans, and personnel costs. These specific costs are dependent on the requirements for protection of an asset and its worth.

The Agency's computer security program is based on the value of assets, estimation of the threat to these assets, and a management committment to protect these assets against threats. The program is not a static one but rather could be described as dynamic, attempting to advance and improve as the computers with which it is involved advance and improve.



Approved For Release 2005/02/10 : CIA-RDP78M02660R000300020014-9